

REMARKS

Reconsideration of the application in light of the above amendments and the following remarks is respectfully requested.

Status of the Claims

Claims 5-15 are pending. Claims 1-2 were previously canceled. Claims 3-4 have been withdrawn from consideration.

Claims 5 and 6 have been amended. Support for the amendments to claims 5 and 6 can be found in the Specification on page 1, paragraph 0003, page 4, paragraph 0014, and page 6, paragraph 0024-0026.

Claims 7-15 have been added. Claims 7-15 are directed to the elected Group II. Support for added claims 7-15 can be found in the Specification on page 5, paragraph 0017 through page 7, paragraph 0026.

No new matter has been added.

Objection to the Specification

The Examiner has objected to the Specification for containing minor informalities. Applicants have amended the Specification to fix minor typographical inaccuracies. Reconsideration and withdrawal of the objection is respectfully requested.

Rejection Under 35 U.S.C. §101

Claims 5 and 6 stand rejected under 35 U.S.C. §101 because the Examiner contends that the claimed invention is directed to non-statutory subject matter. Specifically, the Examiner contends that claims 5 and 6 are directed to methods for establishing a key, the result of which is the

determination of a common key, which produces neither a physical transformation, nor a concrete, tangible, and useful result. The Examiner contends that the methods recited in claims 5 and 6 are directed only to an abstract idea. Applicants respectfully traverse the rejection.

Applicants submit that it is well-known in the art of cryptography that the establishment of a common key has the practical application of allowing the respective subscribers to communicate securely over communication channels while ensuring that only the intended recipient can read the communication. See, Specification, page 1, paragraphs 0002-0003. It is respectfully submitted that an encryption key is useful for transmitting messages over a communication channel. Establishment of a common key for communication as described above is thus a “practical application in the technological arts.” See MPEP §2106 IV.B.2(b)(ii). Therefore, Applicants submit that the methods recited in claims 5 and 6 produce a concrete, tangible, and useful result, as would be apparent to those of ordinary skill in the art.

Notwithstanding the above remarks, Applicants have amended independent claim 5 to recite that the claimed method is “for transmitting messages over a communication channel” and that the encryption key is “useable for transmitting messages over a communication channel.” Applicants submit that using the common key for transmitting messages is a concrete, tangible, and useful result, and therefore the claimed subject matter is statutory.

Reconsideration and withdrawal of the rejection 35 U.S.C. §101 is respectfully requested.

Rejection Under 35 U.S.C. § 112, second paragraph

Claims 5 and 6 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite.

The Examiner contends that the variable “n” has not been defined in the claims. Applicants have amended independent claim 5 to recite that “n” represents the number of subscribers in the group of at least three subscribers.

With respect to the Examiner’s contention specified in the Detailed Action, Item 7, page 4, line 10 through page 5, line 4, the Examiner contends that it is unclear “how each subscriber T_i ($i \neq 1$) has access to the values N_j , where $j \neq 1$. . . Furthermore, it is not clear how the subscriber T_i ($i \neq 1$) have access to the random number z_1 .” (Detailed Action, Item 7, page 4, lines 10-13.) The Examiner contends that “it appears that steps are missing which would provide for the receipt by each subscriber T_i of the values N_j ($j \neq 1$) and also for the receipt or calculation of the symmetric decryption key that would allow decryption of the encrypted random number z_1 .” (Detailed Action, Item, 7, page 4, line 21 through page 5, line 2.) Applicants respectfully traverse the rejection.

Applicants respectfully note that in the method recited in claim 5, it is not necessary for each subscriber T_j ($j \neq 1$) to have direct access to the random number z_1 . As recited in the claim, each subscriber generates a respective message N_j , which is based on a respective random number z_j . Then, each subscriber T_j , $j \neq 1$, transmits its respective message N_j to the first subscriber T_1 , as recited in the “sending the respective message” step of claim 5. After receiving the messages N_j from each of the other subscribers T_j , $j \neq 1$, the first subscriber T_1 creates a respective transmission key k^{ij} for each of the subscribers T_j , $j \neq 1$, as recited in the encrypting step of claim 5. The first subscriber T_1 then sends the encrypted random number z_1 to all the other subscribers T_j , $j \neq 1$, by generating a message M_{ij} . As recited in claim 5, the message M_{ij} is created using “a symmetrical encryption algorithm in which the random number z_1 is encrypted with the transmission key k^{ij} .”

$g^{z_2 z_1}$, respectively. Although T_2 does not actually know the value of z_3 , T_2 has the value of $(g^{z_3})^{z_1}$, and therefore can calculate k . Likewise, although T_3 does not actually know the value of z_2 , T_3 has the value of $(g^{z_2})^{z_1}$, and therefore can calculate k .

Thus, it is clear that each of the subscribers T_j , $j \neq 1$ does not need to have direct access to the random number z_1 , and by having only the encrypted version of z_1 , each of the subscribers T_j is able to calculate the common key k . Applicants submit that claim 5 recites the necessary steps for carrying out the claimed invention, and therefore, is not indefinite.

With respect to the Examiner's rejection regarding the variable " k^{ijn} " recited in claim 6, Applicants respectfully note that claim 6 does not appear to recite such a variable. Applicants submit that claim 6 recites the variable " $k^{ij} = k^{jn}$ " which has been defined in base claim 5. With respect to the Examiner's rejection regarding the feature of "the key" recited in claim 6, Applicants have amended claim 6 to have proper antecedent basis.

In view of the above remarks, Applicant respectfully requests reconsideration and withdrawal of the rejection under 35 U.S.C. §112, second paragraph.

New Claims

New claims 7-15 are directed to subject matter similar to that recited in claims 5 and 6. Support for added claims 7-15 can be found in the Specification on page 5, paragraph 0017 through page 7, paragraph 0026. It is respectfully submitted that new claims 7-15 are patentable.

